REMARKS

Reconsideration and allowance of the subject application in view of the following remarks is respectfully requested.

Claims 1-10, 12-32, and 35-43 are pending.

Reopening of prosecution in view of Applicant's Appeal Brief filed on September 20, 2005 is noted with appreciation.

Rejection of claims 1-10, 12-32, and 35-43 under §103

The rejection of claims 1-10, 12-32, and 35-43 under 35 U.S.C. 103(a) as being unpatentable over Moran (U.S. Patent 6,647,400) in view of Kuznetsov et al. (U.S. Patent 5,483,649) is hereby traversed. The claimed subject matter of claim 1 is patentable over the applied combination of references for at least three reasons.

Claim 1

Moran fails to disclose parsing and comparing parsed records against a template

1. Contrary to the PTO's assertion, Moran fails to disclose the claimed limitation of parsing and comparing parsed records against a template. Moran at column 18, lines 6-58, and at column 32, lines 44-58, fails to disclose parsing the records and comparing the parsed records against a template. Instead, column 18, lines 6-58 of Moran describes the format for message transfers between sensors of the system and the analysis engine. According to Moran, sensor data may be transferred to the analysis engine using the described message header; however, there is no disclosure of comparing parsed records against a template.

Further, column 32, lines 44-58, of Moran discloses cross checking files with signatures of current versions of the file in a database. Moran fails to disclose comparing records against a template according to the description of a template comparison at page 28, lines 20-27 of the

instant specification.

Further still, a file signature is not the same as a template. That is, a file signature cannot be used as a representation of an algorithm to detect a vulnerability exploitation. See e.g., instant specification at page 28, lines 21-24, "[a] detection template is a representation of an algorithm to detect a vulnerability exploitation. ... The template contains logic which will process the kernel event stream." Moran's file signature fails to include logic which will process a record. For either of these reasons, the rejection should be withdrawn.

Kuznetsov fails to disclose reformatting read kernel records

2. Kuznetsov fails to disclose reformatting of read kernel records into a different format as claimed in claim 1. Kuznetsov discloses copying register values, an application program stack indicator, and an application program stack to a memory area used by protection software as part of a protection procedure. Specifically, Kuznetsov "copies the values of the registers used by the original handler," "extracts . . . the value of the application program stack indicator and copies the application program stack to the memory area used by the protection software 20A." Kuznetsov at column 11, lines 50-57. There is no reformatting of read kernel records into a different format. Kuznetsov states that a "stack copy is made" without any disclosure of reformatting of records. There is no disclosure of reformatting of read kernel records in Kuznetsov. For at least this reason, withdrawal of the rejection is respectfully requested.

Moran and Kuznetsov are not combinable

3. Even assuming for the sake of argument that Kuznetsov disclosed reformatting read kernel records into a different format, a person of ordinary skill in the art at the time of the present invention would not have been motivated to combine Kuznetsov with Moran. Kuznetsov is directed to a combined software-hardware-based security system and Moran is directed to a software-based security system. In the background section, Kuznetsov negatively discusses software-based security systems in favor of software-hardware-based security systems. An

object of Kuznetsov is "to provide a personal computer security system having a hardware portion that is not complex." Kuznetsov at column 4, lines 39-41. Kuznetsov discloses "a personal computer . . . with a hardware module that establish[es] a single permitted path . . . that can be monitored and/or obstructed when unauthorized access is attempted to, or a computer virus attempts to write to, the hard disk." Kuznetsov at column 4, lines 17-22. A person of ordinary skill in the art at the time of the present invention would not be motivated to combine the teachings of the applied references.

Further, neither of the combined references teaches or suggests creating "flexibility to read a file on different systems," as set forth in the Office Action. There is no basis in either reference supporting the assertion that a person of ordinary skill in the art would have been motivated to combine the references in order to create flexibility to read a file on different systems. The operation of Kuznetsov would appear to prevent such a flexibility by requiring a hardware module on each different system in order to access the system's hard disks. Further still, as Kuznetsov describes copying register values, an application program indicator, and an application program stack, there is no file to be read on different systems and it is highly unlikely that another system would make use of the copied information.

"When an obviousness determination is based on multiple prior art references, there must be a showing of some 'teaching, suggestion, or reason' to combine the references." Winner International Royalty Corp. v. Wang, 53 USPQ2d 1580, 1586 (Fed. Cir. 2000). The Examiner has failed to make such a showing supporting the applied combination of references and therefore the applied combination of references is improper. The Examiner is in error for any of the above reasons and has not made out a prima facie case of obviousness, and the rejection of claim 1 should be reversed.

For each of the above reasons, claim 1 is patentable over Moran and the rejection should be withdrawn. Claims 2-10 and 12-28 depend, either directly or indirectly, from claim 1, include further important limitations, and are patentable over Moran in view of Kuznetsov for at least the reasons advanced above with respect to claim 1. The rejection of claims 2-10 and 12-28 should be withdrawn.

Claim 9

Additionally, Applicant's remarks regarding claim 9 in view of Moran remain unaddressed. That is, Moran fails to disclose the claim 9 limitation of encrypting information sent between the intrusion detection system and a network. As stated in the instant specification at page 4, lines 5-6, "[e]ncryption is a mathematical technique that prevents the unauthorized reading and modification of data."

Moran at column 16, lines 15-29, describes the passing of values between components of the system by performing data type conversions and not preventing the unauthorized reading and modification of data. Thus, Moran fails to disclose encrypting information transmitted. Additionally, Moran demonstrates a lack of concern for protecting transmissions as at column 10, lines 17-19, Moran "send[s] the extracted information to another (hopefully uncompromised) computer for analysis." Moran fails to disclose encrypting information sent between the detection system and a network. For at least this reason, as well as the reasons advanced above with respect to claim 1 from which claim 9 depends, withdrawal of the rejection is respectfully requested.

Claim 29

The rejection of claims 29-32 and 35-43 as being unpatentable over Moran in view of Kuznetsov is hereby traversed as Moran fails to disclose that if a directory is specifically excluded and a file in the specifically excluded directory is specifically included the file is monitored. Kuznetsov fails to cure the noted deficiencies of Moran. At most, Moran at column 32, line 44-column 33, line 62, describes that "[f]iles in system directories that are not in a package management database or an internal database are flagged as mildly suspicious." The statement relates to how the Moran system handles files which are not in a location at which they are expected to be based on database information regarding the files. There is no disclosure of monitoring a file located in a specifically excluded directory. Moran fails to disclose a specifically included file in a specifically excluded directory and thus cannot disclose monitoring the specifically included file. For at least this reason, the rejection of claim 29 should be withdrawn.

Further, the reasons advanced above with respect to claim 1 and the asserted combination of the applied references are incorporated herein with respect to claim 29.

Claims 30-32 and 35-43 depend, either directly or indirectly, from claim 29, include further important limitations, and are patentable over Moran in view of Kuznetsov for at least the reasons advanced above with respect to claim 29 and the rejection should be withdrawn.

Conclusion

All objections and rejections having been addressed, it is respectfully submitted that the present application should be in condition for allowance and a Notice to that effect is earnestly solicited.

To the extent necessary, a petition for an extension of time under 37 C.F.R. 1.136 is hereby made. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account 07-1337 and please credit any excess fees to such deposit account.

Respectfully submitted,

LOWE HAUPTMAN & BERNER, LLP

Randy A. Noranbrock
Registration No. 42,940

Customer Number: 22429
1700 Diagonal Road, Suite 300
Alexandria, Virginia 22314
(703) 684-1111
(703) 518-5499 Facsimile
Date: February 24, 2006
KMB/RAN/ir